

#4

Docket No.: 62807-032

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Satoshi OSHIMA, et al.

Serial No.:

Group Art Unit:

Filed: February 06, 2001

Examiner:

For: A METHOD AND SYSTEM OF FILE PROTECTION



**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Commissioner for Patents
Washington, DC 20231

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2001-350933, filed November 16, 2001

A Certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Keith E. George
Registration No. 34,111

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 KEG:prp
Date: February 6, 2002
Facsimile: (202) 756-8087

62807-032
OSHIMA et al
February 6, 2002
McDermott, Will & Em

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office

出 願 年 月 日

Date of Application:

2001年11月16日

出 願 番 号

Application Number:

特願2001-350933

ST.10/C]:

[JP2001-350933]

出 願 人

Applicant(s):

株式会社日立製作所

J1011 U.S. PTO
10/066797
02/06/02

CERTIFIED COPY OF
PRIORITY DOCUMENT

2002年 1月18日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 K01011221A

【あて先】 特許庁長官

【国際特許分類】 G06F 3/06

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

 【氏名】 大島 訓

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

 【氏名】 新井 利明

【発明者】

 【住所又は居所】 東京都江東区新砂一丁目 6 番 2 7 号 株式会社日立製作所 公共システム事業部内

 【氏名】 長尾 俊彦

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社日立製作所

【代理人】

 【識別番号】 100075096

 【弁理士】

 【氏名又は名称】 作田 康夫

【手数料の表示】

 【予納台帳番号】 013088

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

【物件名】	要約書	1
【プルーフの要否】	要	

【書類名】 明細書

【発明の名称】 ファイルシステム保護方法及び装置

【特許請求の範囲】

【請求項 1】

揮発性の記憶装置と不揮発性の記憶装置とを備え、一台の計算機上に複数の OS（オペレーティングシステム）を同時に実行させる手段を有する計算機におけるファイルシステム保護方法は、

実行された第 1 の OS が、前記不揮発性記憶装置上の第 2 の OS が利用するファイル群を、揮発性記憶装置上にコピーし、

前記コピーされたファイル群を利用して、前記第 2 の OS を実行させることによって、システムを再起動させる毎に、特定状態のファイルシステムから OS を起動することを特徴とするファイルシステム保護方法。

【請求項 2】

不揮発性記憶装置を備えない OS が、揮発性記憶装置を備えた OS と通信することによって、ファイルを保存することを特徴とする請求項 1 記載のファイルシステム保護方法。

【請求項 3】

前記計算機の前記第 2 の OS が通信装置を備え、かつ、通信装置と不揮発性記憶装置を備えた外部計算機上の OS と前記第 2 の OS とが前記通信装置を介して、ファイルを交換する際に、前記第 2 の OS が前記外部計算機の不揮発性記憶装置上にファイルを保存することを特徴とする請求項 1 及び 2 記載のファイルシステム保護方法。

【請求項 4】

前記第 1 及び第 2 の OS が通信装置を備え、かつ、前記通信装置のそれぞれが通信線で接続され、前記通信装置を介して、ファイルを交換する際に、前記第 2 の OS が前記第 1 の OS の不揮発性記憶装置上にファイルを保存することを特徴とする請求項 1 及び 2 記載のファイルシステム保護方法。

【請求項 5】

前記第 1 及び第 2 の OS が、前記複数の OS を同時に実行させる手段を介して

通信することによってファイルを交換する際に、前記第 2 の OS が前記第 1 の OS の不揮発性記憶装置上にファイルを保存することを特徴とする請求項 1 及び 2 記載のファイルシステム保護方法。

【請求項 6】

揮発性の記憶装置と不揮発性の記憶装置とを備え、一台の計算機上に複数の OS（オペレーティングシステム）を同時に実行させる手段を有する計算機におけるファイルシステム保護装置は、

実行された第 1 の OS が、前記不揮発性記憶装置上の第 2 の OS が利用するファイル群を、揮発性記憶装置上にコピーする手段、

前記コピーされたファイル群を利用して、前記第 2 の OS を実行させることによって、システムを再起動させる毎に、特定状態のファイルシステムから OS を起動する手段を有することを特徴とするファイルシステム保護装置。

【請求項 7】

揮発性の記憶装置と不揮発性の記憶装置とを備え、一台の計算機上に複数の OS（オペレーティングシステム）を同時に実行させる手段を有する計算機におけるファイルシステム保護方法を実行するプログラムを格納した、計算機で読み取り可能な記憶媒体であって、前記方法は、

実行された第 1 の OS が、前記不揮発性記憶装置上の第 2 の OS が利用するファイル群を、揮発性記憶装置上にコピーし、

前記コピーされたファイル群を利用して、前記第 2 の OS を実行させることによって、システムを再起動させる毎に、特定状態のファイルシステムから OS を起動することを特徴とする記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は計算機システムに関し、特にファイルシステムの保護に関する。

【0002】

【従来の技術】

従来の OS（オペレーティングシステム）が持つファイルシステムは、一般に

ファイル単位でのデータの読み込み、書込み、及び実行の可否が設定できるファイル保護の機能を有している。このような、ファイルの読み込み、書込み、及び実行の可否といった情報は、ファイルの属性と呼ばれる。特に、マルチユーザOSが有するファイルシステムには、ユーザ及びグループ毎にファイル単位で属性を設定する機能を有するものもある。

【0003】

OSやアプリケーションの動作に関わる実行プログラムや設定情報は、ファイルシステム内にファイルの形で保存されている。なかでも特に重要なファイルは、通常は読み込み専用の属性を付加して容易に書き換えることが出来ないように運用し、必要に応じて書込みの許可属性を付加することが一般的である。

【0004】

ファイルシステム内に書き込まれたファイルは、システム終了後も不揮発性を有する二次記憶装置内に保存され、システム再起動後再び使用できる。

【0005】

また、あるファイルが更新された場合、ユーザまたはアプリケーション等が更新前の状態を明示的に保存しておかない限り、更新後の状態だけが保存される。

【0006】

【発明が解決しようとする課題】

経験の不足したユーザや不特定多数のユーザがアクセスできる従来のファイルシステムでは、いったん書き込まれたファイルや更新されたファイルを検出し、元の状態に戻すことが困難であるという問題があった。

【0007】

マルチユーザOS（オペレーティングシステム）が有するファイルシステムのように、ユーザごとにファイル属性を設定できる場合、不特定多数のユーザや経験の不足したユーザに対しては、限られたファイルのみに書込みを許し、その他のファイルには更新する権限を付加しないことにより、事前に不用意な書込みを防止することは可能である。しかし、この方法では、教育などのため一時的にファイルにデータを書込む許可を与える必要があるが、その後はファイルの内容を元の状態に戻したいといった要求には応えることができない。

【0008】

また、ユーザごとにファイル属性を設定する機能を持たないファイルシステムにおいては、任意のユーザが自由に属性を変更することができるため、どんな重要なファイルであってもユーザの操作からファイル属性を保護することは難しかった。

【0009】

このような問題を解決するための一つの手法として、システムのある時点の状態を保存しておく、バックアップという手法が用いられる。しかし、バックアップではバックアップしたファイルを元に戻すリストアという処理に手間がかかるため、大規模なシステムではすべてをバックアップして、毎回リストアすることは現実的ではない。

【0010】

【課題を解決するための手段】

本発明は、1台の計算機上で複数のOS（オペレーティングシステム）を同時に実行する際に、第1のOS（バックエンドOS）は、不揮発性二次記憶装置上にファイルシステムを持ち、起動後、自らのファイルシステム内に作成して揮発性記憶装置内に保存しておいた、第2のOS（フロントエンドOS）のファイルシステム（オリジナル）を揮発性記憶装置上にコピーする。バックエンドOSは、揮発性記憶装置上のコピーされたファイルシステムを利用して、フロントエンドOSを起動し、その後のファイル操作もこれを用いる。

【0011】

キーボード、マウス、ディスプレイといったユーザインターフェースは、すべてフロントエンドOS側にもたせるものとする。

【0012】

このような構成をとることで、ユーザが行ったファイル操作は全て、揮発性記憶装置上のファイルシステムに対して行われることとなる。揮発性記憶装置上のファイルシステムは電源断及びシステムリセットで破棄され、再起動後、新たにバックエンドOSからフロントエンドOSにファイルシステムがコピーされるため、システムを再起動するだけで、ユーザが利用するフロントエンドOSは、バ

ックエンドOS内に保存されたバックエンドOSのファイルシステムの状態まで自らのファイルシステムを戻すことが可能である。

【0013】

本発明では、さらに、ファイルシステムが更新された状態を保存した場合に、システムの再起動によって更新された内容が破棄されないように、以下の2つの方法を提供する。

【0014】

第1の方法は、ファイルシステム内の特定のディレクトリやファイルを、OS間の通信機能を利用して、バックエンドOSのファイルシステム内に保存する。システム再起動後、特定ディレクトリやファイルをフロントエンドOS側に書き戻すことで、特定のファイル及びディレクトリの更新内容が保存される。

【0015】

第2の方法は、更新されたファイルシステムの一部または全体を、バックエンドOS側が保持しているオリジナルに反映させる。

【0016】

【発明の実施の形態】

本発明について図面を用いて詳細に説明する。

【0017】

図1は、本発明の実施の形態における計算機101の構成を示す。

【0018】

計算機100は、プロセッサ群110、主記憶装置群120、外部記憶装置群130、通信装置群140、出力装置群150、入力装置群160から構成されている。主記憶装置120は高速ではあるが、高価であり電源を遮断すると記憶内容が失われてしまう（揮発性）。外部記憶装置130は、主記憶装置120と比較して低速ではあるが、安価であり電源を遮断しても記憶内容が失われない（不揮発性）。

【0019】

本発明では、1台の計算機上に複数のOS（オペレーティングシステム）を同時に実行させる、マルチOS構成法を利用する。

【0020】

図2は、本発明の計算機の論理構成を示す概念図である。

【0021】

マルチOSを実現するソフトウェアであるマルチOS構成部230は、以下の特徴を持つ。

【0022】

(1) マルチOS構成部230によって、フロントエンドOS210及びバックエンドOS220が同時に実行される。マルチOS構成部230は、2つのOSが同時に実行するために必要な機能（主記憶分割機能、フロントエンドOSファイルシステムコピー機能等）を有する。

【0023】

(2) フロントエンドOS210及びバックエンドOS220は、それぞれ独立したファイルシステムおよび通信装置を持つ。また、フロントエンドOS210は入出力装置を制御する。

【0024】

(3) マルチOS構成部230は、フロントエンドOSとバックエンドOSの間にOS間通信機能を提供する。

【0025】

図3は、計算機100上の主記憶装置群120が、マルチOS構成部230によって4つの領域に分割された様子を示している。

【0026】

第1の領域は、バックエンドOS主記憶領域310である。この領域はバックエンドOSが動作するための主記憶領域として使用される。

【0027】

第2の領域は、マルチOS構成部領域320である。マルチOS構成部はこの領域を利用してマルチOS構成法を実現する。また、OS間通信機能もこの領域を利用して提供される。

【0028】

第3の領域は、フロントエンドOS主記憶領域330である。この領域は、フ

フロントエンドOSが動作するための主記憶領域として使用される。

【0029】

第4の領域は、フロントエンドOSファイルシステム領域である。ファイルシステムは、通常外部記憶装置に作成されるが、本発明では、フロントエンドOSのファイルシステムは、主記憶装置群120のフロントエンドOSファイルシステム領域340に作成され、フロントエンドOSは第4の領域から起動される。

【0030】

バックエンドOSファイルシステム260は、計算機100の外部記憶装置130に構成される。

【0031】

このような構成をとるため、システム起動時は、バックエンドOS220用のファイルシステムだけが保存されている状態であり、フロントエンドOSのファイルシステムは主記憶装置120に構成されているため、揮発している状態（電源遮断時に内容がリセットされる状態）にある。

【0032】

図4はバックエンドOSファイルシステム260の内部構成を示す。

【0033】

フロントエンドOSファイルシステム260は、マルチOS構成部230が動作するのに必要なファイルであるマルチOS構成部ファイル群430及びバックエンドOS220が動作するのに必要なファイルであるバックエンドOSファイル群420を含んでいる。

次に、図6を用いて、本発明計算機システムの起動手順を説明する。

本発明による計算機システムは図6に示す手順によって起動される。まず、ステップ610で計算機が起動される。続いてステップ620で、バックエンドOSが起動される。次に、ステップ630でマルチOS構成部が起動される。そして、ステップ640でフロントエンドOSファイルシステムがコピーされ、最後に、ステップ650においてフロントエンドOSが起動される。

【0034】

上記の手順を、図5を用いてさらに詳しく説明する。

【 0 0 3 5 】

ステップ 6 1 0 で計算機が起動されると、ステップ 6 2 0 にしたがって、計算機は外部記憶装置 1 3 0 に配置されたバックエンド OS ファイルシステム 2 6 0 中のバックエンド OS ファイル群 4 2 0 から、バックエンド OS 2 2 0 を起動する (5 1 0) 。

【 0 0 3 6 】

続いて、ステップ 6 3 0 に従って、バックエンド OS 2 2 0 は、自身のファイルシステム 2 6 0 に配置されたマルチ OS 構成部ファイル群 4 3 0 から、マルチ OS 構成部 2 3 0 を起動する (5 2 0) 。このときマルチ OS 構成部 2 3 0 は、主記憶装置 1 2 0 を、図 3 で示された領域に分割する。

【 0 0 3 7 】

そして、ステップ 6 4 0 に従い、バックエンド OS 2 2 0 はバックエンド OS ファイルシステム 2 6 0 に配置された、フロントエンド OS ファイル群 4 1 0 の全てを、マルチ OS 構成部 2 3 0 を利用して、主記憶装置 1 2 0 のフロントエンド OS ファイルシステム領域 3 4 0 にコピーする (5 3 0) 。フロントエンド OS ファイルシステム領域 3 4 0 は、主記憶装置 1 2 0 にあるため計算機が起動された際に初期化されている。

【 0 0 3 8 】

最後に、ステップ 6 5 0 に従い、マルチ OS 構成部 2 3 0 はフロントエンド OS ファイルシステム 2 5 0 にコピーされたフロントエンド OS ファイル群 5 5 0 を利用して、フロントエンド OS 2 1 0 を起動する (5 4 0) 。

【 0 0 3 9 】

起動後、フロントエンド OS 2 1 0 が実施するファイル操作は主記憶装置 1 2 0 のフロントエンド OS ファイルシステム 2 5 0 に対して行われ、バックエンド OS ファイルシステム 2 6 0 のフロントエンド OS ファイル群 4 1 0 には影響を与えないため、本発明の方法を用いて構成された計算機システムのフロントエンド OS 2 1 0 は、定められたファイルシステムの状態から起動することが可能となり、フロントエンド OS 2 1 0 起動後にフロントエンド OS ファイルシステム 2 5 0 に対して行われたファイル操作は、システム再起動後に揮発される (リセ

ットされる)。

【0040】

計算機に備えられた入出力装置150は、全てフロントエンドOSで使用するよう、計算機を構成することにより、計算機の起動後にユーザが行う操作は全てフロントエンドOSに対して行われるようになるため、計算機を毎回同じ状態で起動したい場合に有効である。

【0041】

これまで説明してきた方法により、同じファイルシステムの状態で計算機システムを起動することが可能となった。しかし、これだけでは計算機を使用して作成した情報を保存しておくことが出来ない。そこで、本発明では情報を保存する方法を用意する。

【0042】

本発明においてフロントエンドOS上で作成したファイルを保存する方法の一番目として、通信装置を介して、ファイルを保存する方法を用意する。

【0043】

図7は、これまでの説明に用いた計算機に、もう一台の外部の計算機を接続した構成を示す。

図7において、フロントエンドOS210は、通信装置270を備える。また、外部の計算機710は、不揮発性記憶装置と通信装置730を備える。フロントエンドOS210が備える通信装置140と計算機710が備える通信装置730は、通信線740で接続されている。計算機710は、通信によって自身が備える不揮発性記憶装置に作成したファイルシステムに対し、フロントエンドOS210がファイルを書き込むことを許す機能を提供する。これを共有と呼ぶ。

【0044】

フロントエンドOS210の使用者は、揮発させずに保存したいファイルについては、この共有を利用して計算機710側にこのファイルを保存することにより、フロントエンドOSを再起動しても初期化されずにファイルを残すことができる。

【0045】

図8は、フロントエンドOS 210及びバックエンドOS 220がそれぞれ通信装置270及び通信装置280を備えた計算機を示す。

【0046】

図7と同様に、フロントエンドOS 210は通信装置270を介してファイルを共有する。ただし、図8における計算機では、フロントエンドOS 210とバックエンドOS 220が通信装置270を介して通信し、バックエンドOSファイルシステム260内に、フロントエンドOSファイル群810としてファイルを保存する。これにより、1台の計算機だけでフロントエンドOS 210のファイルシステムを保護しつつ、指定したファイルを保存することができる。

【0047】

図9は、フロントエンドOS 210及びバックエンドOS 220がマルチOS構成部230を介して通信する機能を備えた計算機を示す。

【0048】

図7や図8と同様に、フロントエンドOS 210はマルチOS構成部230を介してファイルを共有する。ただし、図9における計算機では、フロントエンドOS 210とバックエンドOS 220がマルチOS構成部230を介して通信し、バックエンドOSファイルシステム260内に、フロントエンドOSファイル群910としてファイルを保存する。これにより、1台の計算機だけで通信装置を使用することなくフロントエンドOS 210のファイルシステムを保護しつつ、指定したファイルを保存することが可能となる。この方法は、フロントエンドOSやバックエンドOSが通信装置を制御する機能やファイルを共有する機能を備えていない場合でも適用することができる。

【0049】

さらに、図8や図9の方法を利用して、フロントエンドOSファイルシステムの一部を保存するだけでなく、図5のフロントエンドOSファイル群410をも更新できる計算機システムを構築できる。これにより、フロントエンドOSファイルシステム更新の全体を、バックエンドOSファイルシステムに含まれる元のファイル群に反映させることもできる。

【0050】

以上に述べた本発明のファイルシステム保護法方を実行するプログラムを、計算機で読み取り可能な記憶媒体に格納し、実行時に読み込んで本発明を実施することもできる。

【0051】

【発明の効果】

本発明によれば、ファイルシステムに対して行われた変更を、システム再起動により無効化することができる。

【0052】

この特長を利用して、例えば、不特定多数の人が触れる可能性のある展示用計算機にこのシステムを適用することで、システムに対して行われた変更を無効化し、動作することが確認されている状態に復元することで、システムを安定運用することが可能となる。また、システム管理を修得するための演習の際に利用することで、アプリケーションのインストールやシステムの設定変更といった、システムに障害を発生させる危険のある行為を、安全に行うことができる。

【0053】

さらに、管理者が認めた変更については、これを保存することもできるため、ユーザが定められたアプリケーションで作成したデータは保存しつつ、その他に管理者の指示に反してインストールされたアプリケーションは取り除くといった運用が可能となる。これにより、システム管理者の運用管理コストを大幅に低下できる。

【0054】

また、ファイルシステムに対して行われた変更全体を保存することもできるため、システムに障害を発生させる危険のある行為を行った後、十分安全性を確認してから、その変更を保存するといった、計算機の利用が可能となる。

【図面の簡単な説明】

【図1】

計算機のハードウェア構成である。

【図2】

計算機システム構成である。

【図 3】

主記憶装置の内部構成である。

【図 4】

外部記憶装置の内部構成である。

【図 5】

起動時のシステム構成である。

【図 6】

起動手順である。

【図 7】

外部に計算機を伴ったファイル保存の例である。

【図 8】

通信装置を介してバックエンド OS ファイルシステムにファイルを保存する例である。

【図 9】

マルチ OS 構成部を介してバックエンド OS ファイルシステムにファイルを保存する例である。

【符号の説明】

1 1 0 : CPU、1 2 0 : 主記憶装置、1 3 0 : 外部記憶装置、

1 4 0 : 通信装置、1 5 0 : 出力装置、1 6 0 : 入力装置、

2 1 0 : フロントエンド OS、2 2 0 : バックエンド OS、

2 3 0 : マルチ OS 構成部、2 4 0 : 入出力装置、

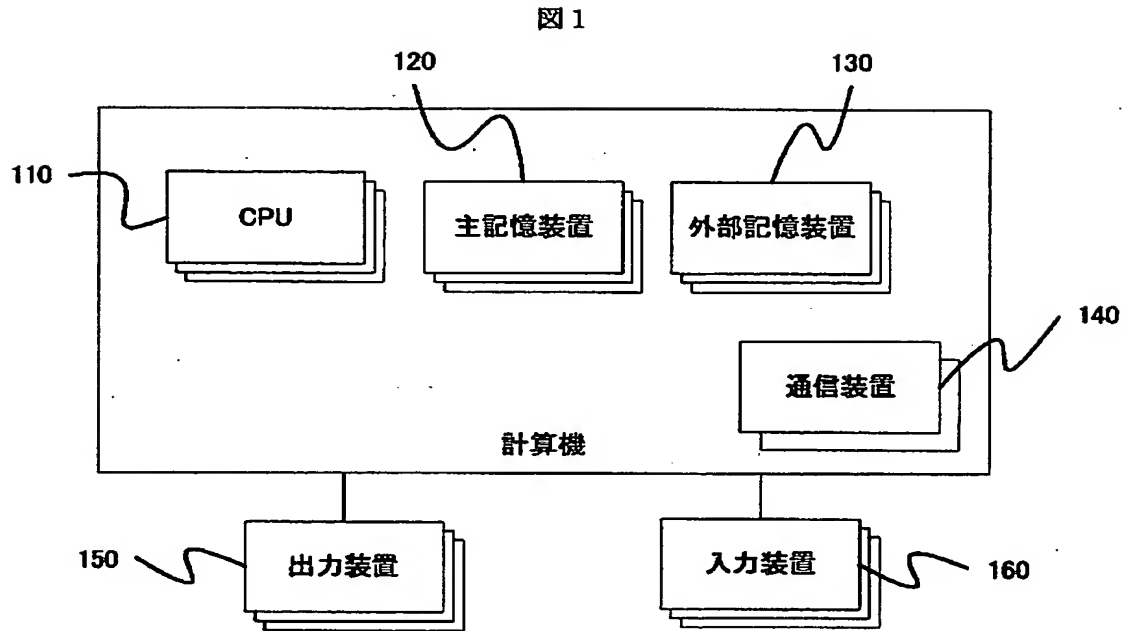
2 5 0 : フロントエンド OS ファイルシステム、

2 6 0 : バックエンド OS ファイルシステム、

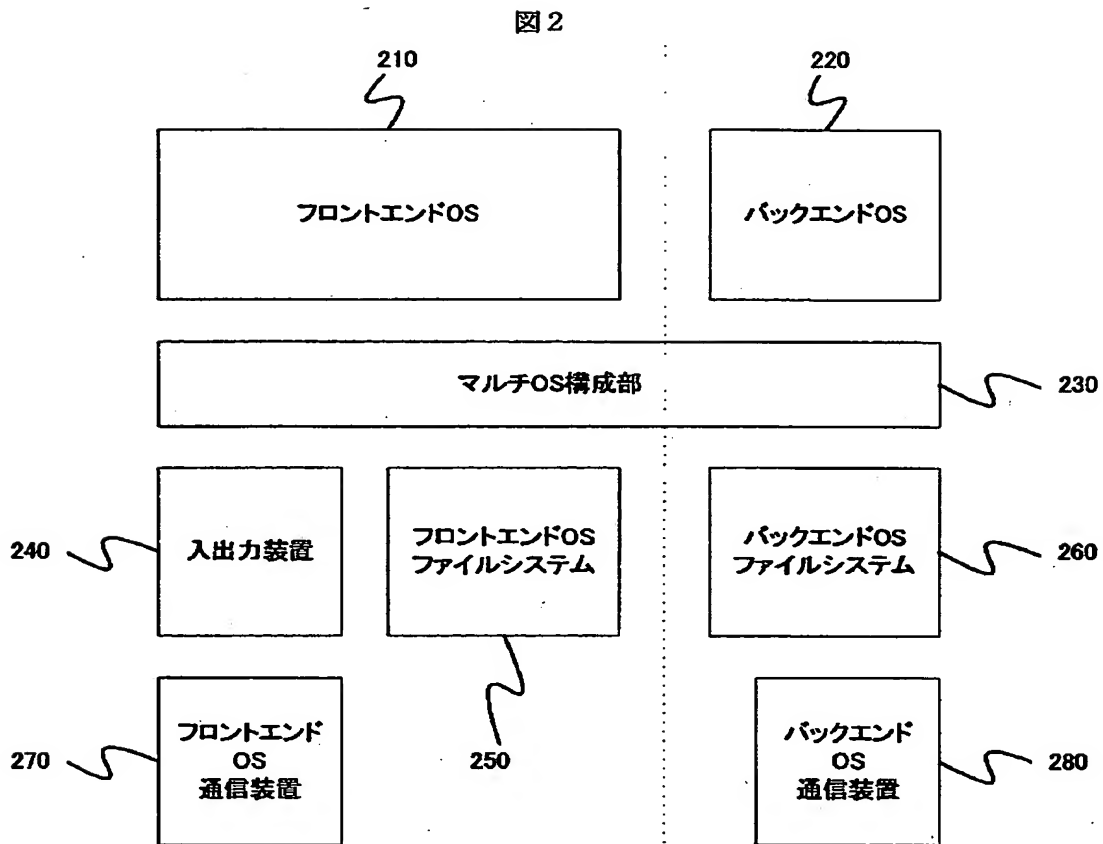
2 7 0 : フロントエンド OS 通信装置、2 8 0 : バックエンド OS 通信装置

【書類名】 図面

【図 1】

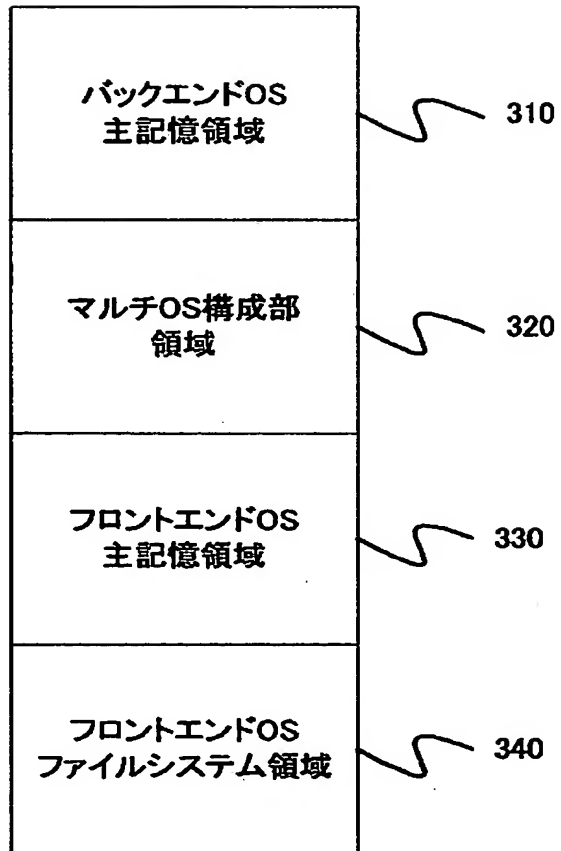


【図2】



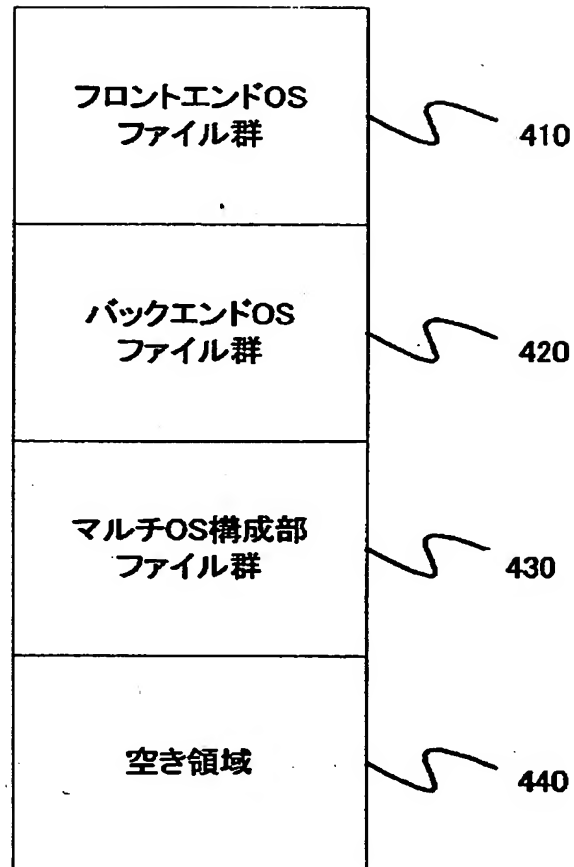
【図3】

図3



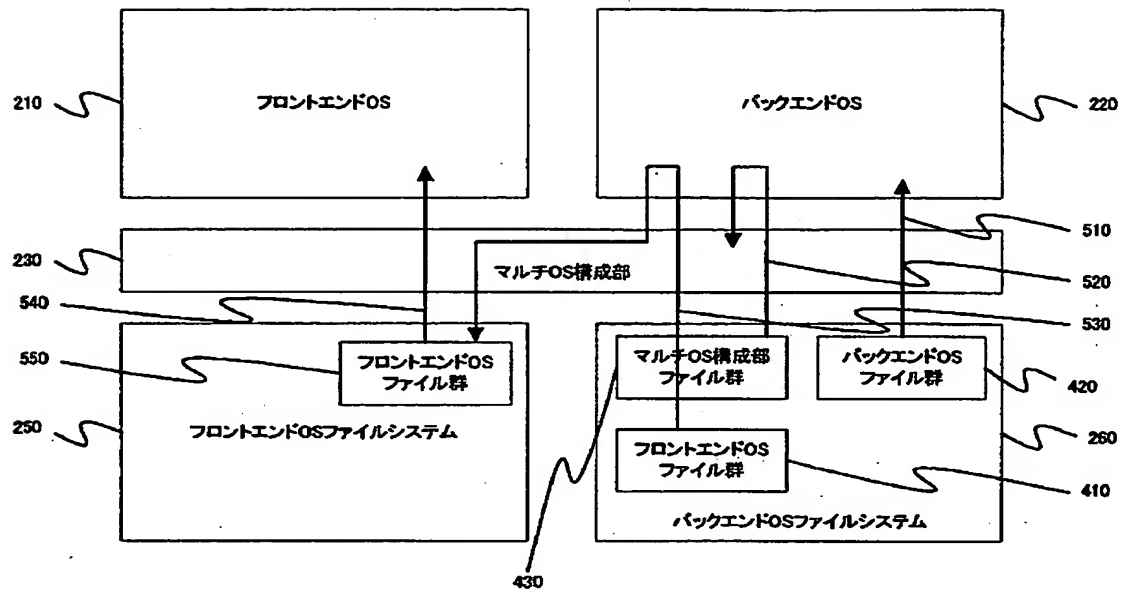
【図 4】

図 4



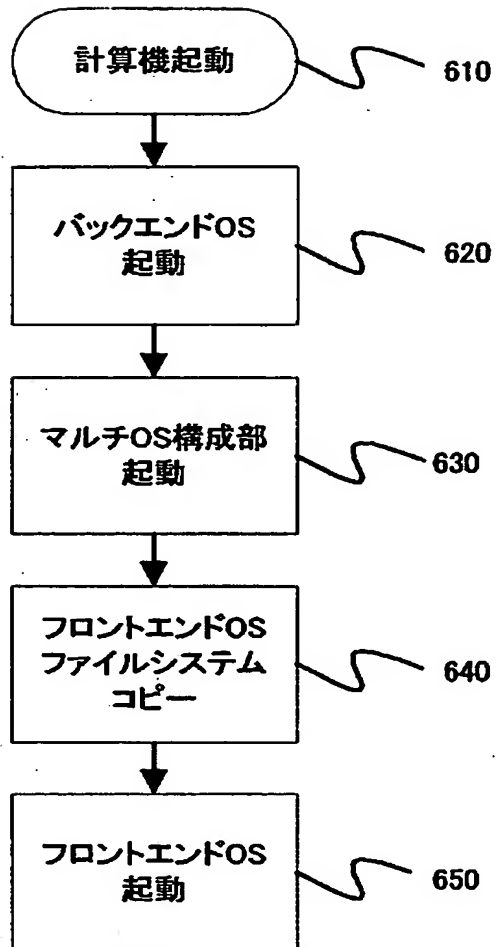
【図5】

図5

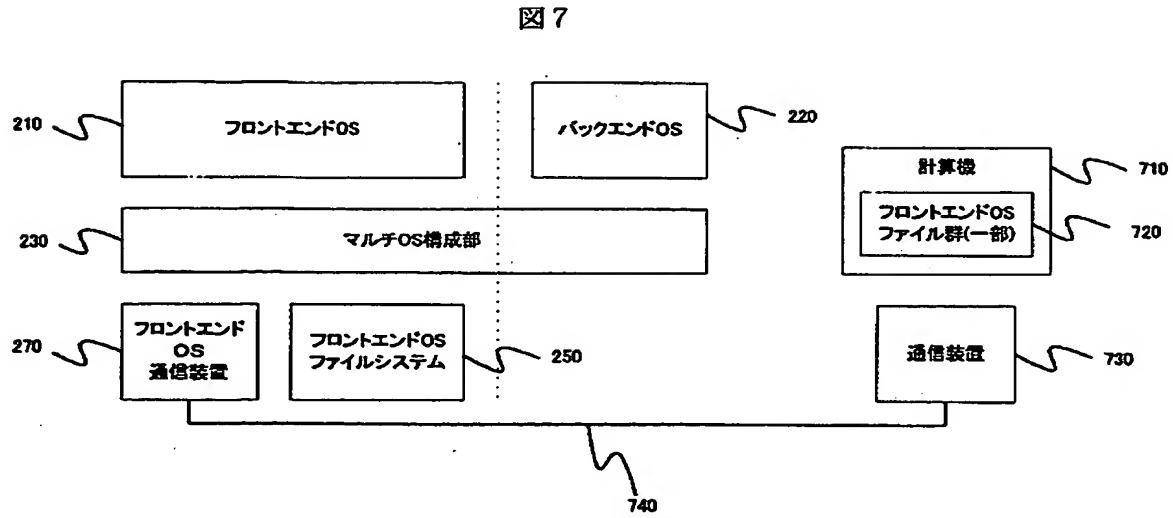


【図 6】

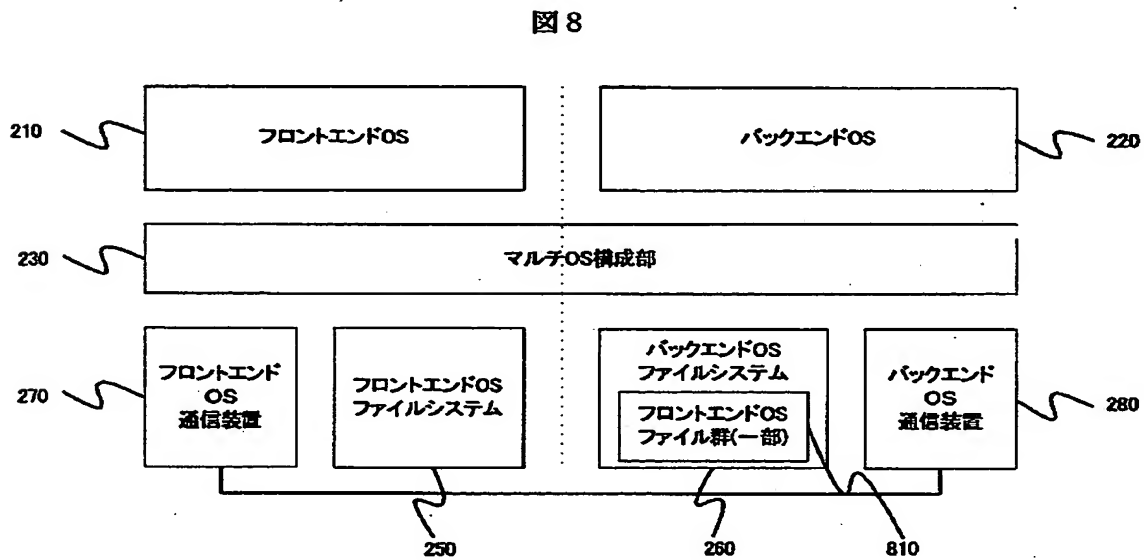
図 6



【図 7】

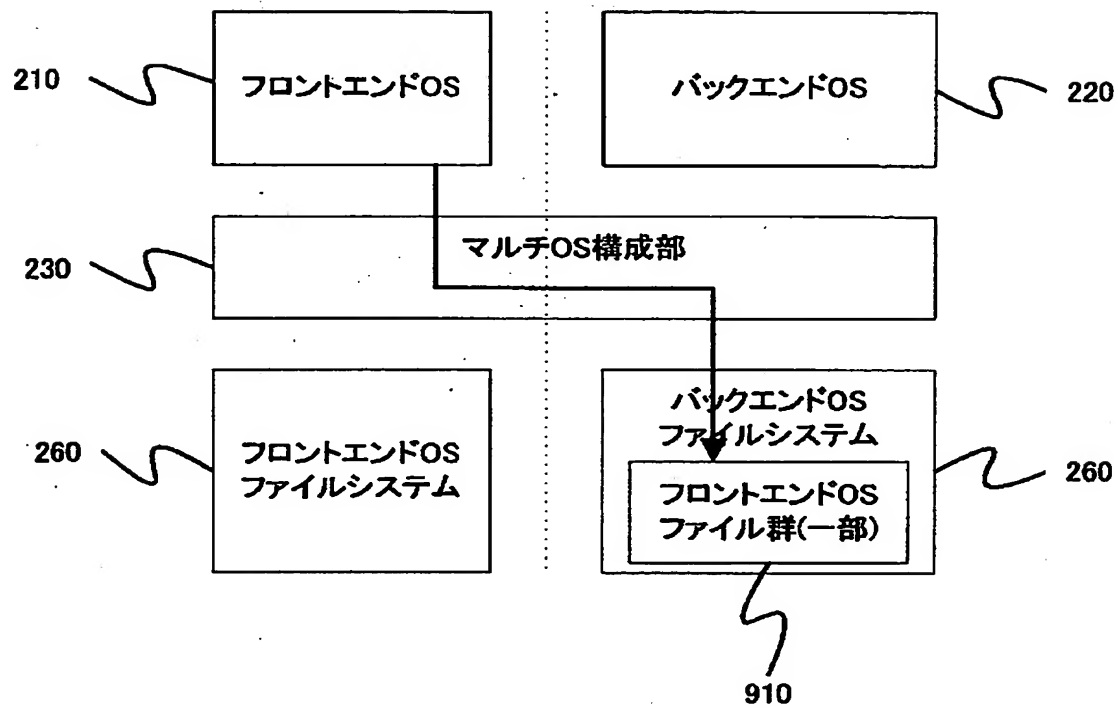


【図 8】



【図 9】

図 9



【書類名】 要約書

【要約】

【課題】

従来のファイルシステムでは、経験の不足したユーザや不特定多数のユーザが触れるシステムでは、いったん書き込まれたファイルや更新されたファイルを検出し、元の状態に戻すことが困難である。

【解決手段】

1 台の計算機上で複数のOSを同時に実行する際に、ファイルシステム内の特定のディレクトリやファイルをOS間の通信機能を利用して、バックエンドOSのファイルシステム内に保存する。システムの再起動後、特定ディレクトリやファイルをフロントエンドOS側に書き戻すことで、特定のファイル及びディレクトリの更新が保存される。更に、更新されたファイルシステムの一部または全体を、バックエンドOS側が保持しているオリジナルに反映させる。

【選択図】 図5

認定・付加情報

特許出願の番号	特願2001-350933
受付番号	50101688433
書類名	特許願
担当官	第七担当上席 0096
作成日	平成13年11月19日

<認定情報・付加情報>

【提出日】	平成13年11月16日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地
氏 名 株式会社日立製作所